REMARKS

Applicants respectfully request reconsideration of the rejection of this application as examined pursuant to the office action of April 5, 2006. In the office action, Claims 1-40 were examined. Independent Claims 1, 11, 18 and 27 have been amended. Claims 32-40 have been cancelled from consideration in this application. Claims 1-31 remain pending.

Claims 1-40 were rejected in the office action under 35 USC § 103(a) as being unpatentable over US Patent No. 6,122,664 issued to Boukobza et al. ("Boukobza") in view of the published US Application Publication No. 2004/0107362 to Ravishankar et al. ("Ravishankar").

The Applicants have previously noted that the independent claims of the present invention are directed to adjusting the policies associated with the usage of network services available for an attached function. Independent Claims 1 and 11 describe a step of the method of the invention as modifying by one or more devices of the network infrastructure the static policies, the dynamic policies, or both for the attached function based upon the detection of one or more triggers. Independent Claims 18 and 27 describe a feature of the system of the invention that the dynamic policy function module of the network infrastructure sets static and dynamic policies for the attached function, monitors the network system for triggers, and modifies the static policies, the dynamic policies, or both for the attached function based upon the detection of one or more triggers.

Applicants have additionally amended the identified independent claims to further distinguish the present invention from the cited reference combination. Specifically, each has been amended to describe the present invention as either a method or system for controlling network system usage by an attached function through direct modification by one or more devices of the network infrastructure of static and/or dynamic policies for the attached function without manual intervention by a network administrator. Applicants respectfully note that the prior art fails to teach or describe direct policy modification upon the detection of a trigger without manual intervention.

In all independent claims, therefore, it is the entitlement of the particular attached function to use the network services that is established by the interaction of the detection of a trigger and the modification directly through one or more devices of the network infrastructure of

one or more usage policies. Applicants respectfully suggest that the reference previously cited and the newly cited reference fail to teach these combinations of features. Further, for purposes of clarification regarding the present invention in comparison to the cited references, policies are permissions of access. They are not parameters, which are conditions monitored for changes, which condition changes may result in policy changes. In addition, policies are not rules of operation but instead comprise rules, and in fact, a single policy may comprise many rules. The present invention is a direct function for changing through network devices policies (thereby one or more in a set of rules) for an attached function based on conditions (parameters) monitored.

The 35 USC § 103(a) Rejection

Claims 1-40 were rejected in the April 5, 2006, office action as being unpatentable over Boukobza in view of Ravishankar. Claims 1-31 are currently pending. It is stated in the office action, among other things, that Boukobza teaches setting and modifying static and dynamic policies. Column 2, lines 21-36 and column 3, line 60 to column 4, line 5, are cited for this position. However, a careful review of these passages and the remainder of the text of the Boukobza reference clearly indicate that static and dynamic parameters are contemplated, not policies. Boukobza describes parameters as values or conditions to be monitored for, whether they are static or dynamic parameters. These parameters correspond to conditions of operation.

Applicants respectfully note that Boukobza makes no mention of policies, which are the permissions granted to attached functions for usage of network services. For example, the policy of allowing access to engineering applications may be granted to one attached function, while another attached function may be permitted access to accounting applications through a different policy. The present invention changes established policies for an attached function directly by the network infrastructure based on triggers. Those triggers may be the result of particular actions of an attached function, the actions of other attached functions, or other conditions of operation of the network infrastructure. The independent claims of the present invention are directed to policy changes. Boukobza is directed to monitoring for triggers. Boukobza is not directed to automated policy changes based upon the detection of triggers, and instead teaches away from such a characteristic. Specifically, Boukobza states in the abstract and column 2, lines 36-38, thereof calls for "possibly initiating actions associated with these tested conditions, which parameters, conditions and actions are modifiable by the user of the management node.

In the April 5, 2006, office action, the examiner notes that Boukobza fails to teach modifying by one or more devices of the network infrastructure policies for the attached function based upon the detection of triggers. That is understandable since the most favorable reading of Boukobza is that it provides for monitoring conditions that could result in triggers. The examiner now asserts that the Ravishankar reference teaches a system and related method for modifying static and dynamic policies based on the detection of triggers. The examiner specifically asserts that the Ravishankar reference is relevant art. Applicants respectfully disagree with the assertions that a) Ravishankar is relevant art; b) Ravishankar teaches direct modification through one or more devices of the network infrastructure of network usage by attached functions; and c) Ravishankar does so directly for attached functions based on triggers.

Ravishankar is limited to a telecommunications system. That is, the internal switching system of a public telephone network for land and cellular lines using the SS7 signaling protocol. It is not directed to the broader type of data networking infrastructure of the type associated with the present invention. Therefore, Ravishankar is not applicable to the present invention and cannot be combined with the Boukobza reference. Moreover, the type of events that are characterized as triggering events by Ravishankar are based on localized conditions and not system-wide conditions. That is, the triggering condition is based solely upon the signal received at a particular module rather than upon any type of system-wide event. The present invention is not limited to such a triggering condition.

While Ravishankar uses the word "policies" in paragraphs [0035] and [0036] thereof, Applicants respectfully suggest that Ravishankar is actually describing rules as defined in the present application. That is, the examples of changes resulting from trigger detections appear to be directed to specific operational modifications (such as blocking, notifying, "throttling" and confirming) rather than actual policy adjustments (such as, for example, this attached function is no longer permitted to access the corporate database). Nevertheless, whether the Ravishankar policies are arguably equivalent to the policies defined in the present application (which Applicants respectfully contends they are not) the reference fails to teach that any policy modifications are made directly by one or more network infrastructure devices. Ravishankar makes no mention of direct modification.

In the context of the telecommunications system to which Ravishankar is limited, it is clear that any "policy" modifications are made manually by a network administrator. See, for

example, the last sentence of paragraph [0036] of Ravishankar, which states that dynamic enforcement "policies" may be changed on-the-fly by a telecommunications provider. It is understood from a complete review of Ravishankar that the reference describes administrative domains, with the telecommunications provider establishing umbrella static "policies" of the entire system, and individual service providers having lesser authority to change sub "policies," referred to as "on-the-fly" modifications. In either instance, it is the network administrator who makes the changes upon examination of a triggering condition. On the other hand, the present invention enables direct policy modification for an attached function by one or more network infrastructure devices without requiring any intermediary intervention by a network administrator.

It can also be seen from Fig. 2 and paragraphs [0035] and [0036] of Ravishankar that triggering rules and "policies" are embodied discreetly in the individual communication module. On the other hand, the system and related method of the present invention are not limited to the detection and storage capacity of an individual network infrastructure device. Further, Ravishankar teaches in paragraph [0037] that the screening provided by the trigger evaluation system of paragraphs [0035] and [0036] is preferably hierarchical; that is, the screening of a particular message may occur in stages, and particularly manual intervention via the network administrator, resulting in overall network slowdown and reduced responsiveness to attached function queries. Further, there is no indication that Ravishankar provides for direct "policy" change for an attached function. Instead, it may be directed to global changes for an interconnection device affecting all attached functions of that device, whether the triggering condition is applicable to some or all of them. The present invention, on the other hand, provides for decision making and enforcement with respect to an attached function directly at the network infrastructure device based on policies specific for that attached function. In particular, Ravishankar shows that the detection of a trigger either blocks the incoming telephone signal, notifies the network operator (the system management), "throttles" as described therein, seeks guidance form the network administrator, or simply logs the message. That is, in all instances, the module of the Ravishankar system receiving a telephone signal does modify the network usage by an attached function. The present invention specifically provides that functionality directly through one or more network infrastructure devices as described in the pending claims.

Applicants further note that dependent Claims 2-7, 12-15, 20-22, 25, and 29 are directed to storing or caching policy histories and using them in various ways to establish policies and/or triggering conditions. Boukobza is cited in the April 5, 2006, office action as apparently teaching such policy history storage and usage. However, the portions of the Boukobza cited in the rejections of those claims fail to make any reference to policy storage, and further fail to associate policy histories stored with policy changes for attached functions. As earlier noted, Boukobza is not even directed to policies. Instead, it is related to parameters used to define triggering conditions. The Ravishankar reference makes no mention at all of policy storage and usage of policy history in establishing policies. The present invention describes such features in a portion of the pending claims.

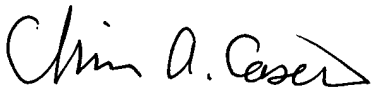
Claim 10 was rejected based on the asserted teachings of the abstract of the Boukobza reference. However, a review of that abstract makes clear that Boukobza makes no mention that the only static policies are dynamic policies. In fact, Boukobza makes no mention at all of policies in the abstract. It is also noted that the Ravishankar reference fails to teach such a relationship between static and dynamic policies. The present invention describes such a feature in pending Claim 10.

The present invention is directed to static and/or dynamic policy changing directly by one or more devices of the network infrastructure based on monitored triggers. The triggers may be most any condition or change of condition of the network system. Boukobza may be a means to employ autonomous agents to monitor for triggers. However, Boukobza fails to describe what to do with the information obtained through use of the autonomous agents. Ravishankar is simply not applicable to the present invention in that it is limited to telephonic exchanges, restricts action to only triggers associated with a particular network device, and does not enact policy changes directly by one or more network infrastructure devices with respect to an attached function. The present invention is an automated system for changing policies, or permissions of network system usage, for attached functions based on the triggers detected. In view of the arguments presented herein, Applicants respectfully suggest that the 35 U.S.C. § 103(a) rejection of pending Claims 1-31 has been successfully traversed. Withdrawal of that rejection is therefore requested.

CONCLUSION

Applicants respectfully request entry of these remarks into the record in view of the newly cited reference and suggest that the rejection under 35 § 103(a) has been successfully traversed. Allowance of pending Claims 1-31 is therefore requested.

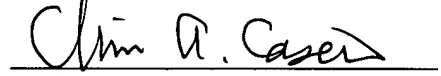
Respectfully submitted,



Chris A. Caseiro, Reg. No. 34,304
Attorney for Applicants
Verrill & Dana, LLP
One Portland Square
Portland, ME 04112-0586
Tel. No. 207-253-4530

Certificate of Express Mailing

I hereby certify that this correspondence is being deposited with the U.S. Postal Service using the Express Mail Service in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450, on September 5, 2006, Express Mail label no. EQ357089105US. It is hereby requested that this filing be granted a filing date of September 5, 2006.



Chris A. Caseiro